AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A ~~computer/network interface~~device for interfacing between a computer and a network, said device being pluggable into a computer, said device comprising:

a first external hardware interface for pluggable connection to external hardware, said first interface being physically disposed in said device for receiving data from a first zone in a first zone data format;

means disposed within said device for processing said received data through performance of a cryptographic operation on at least a portion thereof;

a second external hardware interface for pluggable connection to external hardware, said second interface being disposed in said device for sending said processed data to a second zone in a second zone data format;

one of said interfaces being plug-in connectable to a host computer system; and

means disposed within said device arranged to pass said processed data exclusively from said processing means to said second external hardware interface within said device.

2. (Previously Presented) A computer/network interface device as in claim 1 further comprising:

means disposed within said device arranged to convert said received data in said first zone data format into at least one data format other than said first zone data format prior to said data processing.

3. (Previously Presented) A computer/network interface device as in claim 1 further comprising:

means disposed within said device arranged to transform the data format of said received data from said first zone at least twice prior to said data processing.

4. (Previously Presented) A computer/network interface device as in claim 1 in which said first zone data format is packetized data, said device further comprising:

means disposed within said device for reading at least one item of identification data from each packet;

wherein said processing means is arranged to process each respective packet in dependence on each corresponding item of identification data.

5. (Currently Amended) A computer/network interface device as in claim 4 further comprising:

a store located within said device for storing one or more rules, each rule being linked with at least one of item of identification data;

wherein said processing means is arranged to process each packet in dependence upon the rule linked with the corresponding item(s) of identification data.

6. (Previously Presented) A computer/network interface device as in claim 1 wherein one of the first and second external hardware interfaces is suitable for connection to said host such that the data format utilized by such a connected interface is one utilized by the host.

7. (Previously Presented) A computer/network interface device as in claim 5, wherein one of the first and second external hardware interfaces is suitable for connection to said host such that the data format utilized by such a connected external hardware interface is one utilized by the host in which, in response to receiving at least one control packet including at least an item of control identification data and control instructions through the other external hardware interface which is not connected to the host and reading said item of control identification data from a control packet, said processing means is arranged to change said rules in said store in dependence upon said corresponding control instructions.

8. (Currently Amended) A ~~computer/network interface~~ device for interfacing between a computer and a network, said device being pluggable into a computer, said device comprising:

a first external hardware interface for connection to external hardware, said first interface being disposed in said device for receiving data from a first authorized party in a first data format;

means disposed within said device for processing said received data through performance of a computational operation on at least a portion thereof;

a second external hardware interface for connection to external hardware, said second interface being disposed in said device for sending said processed data to a second authorized party in a second data format;

means disposed within said device arranged to pass said processed data exclusively from said processing means to said second external hardware interface within said device;

wherein said operation performed by said processing means is such that if said sent processed data is intercepted by an unauthorized party, the recovery of said received data from said processed data is computationally unfeasible.

9-24. Cancelled.

25. (New) A method for interfacing between a host computer and a network using a device that is pluggable into said computer, said method comprising:

providing a device having a first external hardware interface physically disposed in said device for receiving data from a first zone in a first zone data format and a second external hardware interface disposed in said device for sending said processed data to a second zone in a second zone data format;

connecting one of said interfaces to a said host computer system and the other of said interfaces to a network;

processing said received data entirely within said device through performance of a cryptographic operation on at least a portion thereof; and

passing said processed data exclusively from said processing step to said second external hardware interface within said device.

26. (New) A method as in claim 25 further comprising:

converting within said device said received data in said first zone data format into at least one data format other than said first zone data format prior to said data processing.

27. (New) A method as in claim 25 further comprising:

transforming within said device the data format of said received data from said first zone at least twice prior to said data processing.

28. (New) A method as in claim 25 in which said first zone data format is packetized data, said method further comprising:

reading within said device at least one item of identification data from each packet;

wherein said processing step is arranged to process within said device each respective packet in dependence on each corresponding item of identification data.

29. (New) A method as in claim 28 further comprising:

storing within said device one or more rules, each rule being linked with at least one of item of identification data;

wherein said processing step is arranged to process each packet in dependence upon the rule linked with the corresponding item(s) of identification data.

30. (New) A method as in claim 25 wherein the data format utilized by the interface connected to the host computer is a data format utilized by the host computer.

31. (New) A method as in claim 29 wherein the data format utilized by the interface connected to the host computer is a data format utilized by the host computer;

wherein, in response to receiving at least one control packet including at least an item of control identification data and control instructions through the external hardware interface which is not connected to the host computer, and reading said item of control identification data from a control packet, said processing step is arranged to change rules stored in said device in dependence upon said corresponding control instructions.

32. (New) A method for interfacing between a computer and a network with a device that is plugged into a computer, said method comprising:

providing a device having a first external hardware interface for receiving data from a first authorized part in a first data format and a second external hardware interface for sending said processed data to a second authorized party in a second data format;

connecting said hardware interfaces between said computer and said network; and

processing within said device said received data through performance of a computational operation on at least a portion thereof;

passing said processed data within said device exclusively from said processing step to said second external hardware interface;

wherein said processing step is such that if said sent processed data is intercepted by an unauthorized party, the recovery of said received data from said processed data is computationally unfeasible.